COMPUTER NEWS from the

MAY 2013 Volume 1 NO. 5

As found on the web and other sources

Windows Blue: Microsoft May Resurrect Start Button

- By Brandon Dimmel on 20130418 in “Infopackets.com”.

According to a new report, Microsoft may be considering reviving the Windows Start Button with the release of Windows Blue, its next major update for the Windows 8 operating system (OS).

The report comes to us from ZDNet's Mary Jo Foley, a prominent industry insider with sources at Microsoft.

Foley says she's learned that Microsoft may bring back not just the Start Button -- a landmark navigation tool found in virtually every single previous Windows operating system -- but also the ability to boot straight to the desktop. (Source: pcworld.com)

If true, this would mean a major overhaul of Windows 8's user interface.

Microsoft Maintains Live Tiles "Easy" to Learn

The operating system caused quite a stir by effectively forcing users to employ a new "Live Tiles" user interface (UI) that is designed with mobile devices (like tablet computers and smartphones) in mind.

Criticism abounded but Microsoft officials have insisted that the Live Tiles UI is "easy to start to learn."

Like many Windows 8 users, Foley isn't buying Microsoft's argument. "I, myself, have adapted to the new UI well on my touch-screen Surface RT," she says.

"But like a number of business users, I find the new UI more of a curse on non-touch-screen machines. As a result, I am still running Windows 7 on two of my three Windows devices." (Source: zdnet.com)

Obviously, the return of the Windows Start Button and automatic booting to the desktop would introduce huge changes to Windows 8. More importantly, it would also be an indirect admission by Microsoft that it went too far too fast with the new Live Tiles interface.

Nevertheless, Foley says that at least one of her sources has confirmed that Windows Blue will bring these hallmark Windows features back to life.

Windows Blue Expected Later This Summer

Of course, Foley admits that, at this point, nothing is for certain. "It's not 100 percent sure that either / both of these options will be baked into the final Blue release, which is expected to be released to manufacturing on or around August 2013," she said.

Although Windows Blue (which is also known as Windows 8.1) isn't expected to be released until at least late summer 2013, a Windows Blue Preview could be available by June. (Source: zdnet.com)

That should provide us with some indication as to where Microsoft is headed with this new and somewhat mysterious new update.

BOTNET ALERT:

Are You Vulnerable?

From “askbobrankin.com”

How easy is it to take over hundreds of thousands of computers, and enslave them in a botnet that could be used by hackers for malicious purposes? Not so hard, it turns out. Last year, an anonymous researcher created software of the type used by hackers, and within one day, created a botnet of over 400,000 computers. He kept the botnet alive for four months, and nobody noticed. Here's what you need to know about botnets...

What is a Botnet?

Perhaps you've read warnings about your computer getting caught up in a botnet, but you don't really understand the danger. I'll explain in simple terms what a botnet is, how it can affect your computer, and how to avoid them.

Okay, here's the scoop... a botnet is a collection of ordinary home and office computers that have been compromised by rogue software. The term "botnet" is short for "robot network" and describes the situation rather well. Computers that have been caught up in a botnet have been effectively taken over, and can be used to perform almost any task by the person or persons who control the botnet. Botnets are controlled by criminals and other miscreants whose motives include selling products, operating financial scams and crippling websites through coordinated attacks.

> Should you be concerned about botnets? Yes, because botnets operate silently, and your computer may be affected without you ever suspecting it. Botnets are everywhere. It is estimated that over 30 million "zombie" computers are unknowingly caught up in these networks that distribute spam, steal personal information and participate in denial of service attacks.

Botnets are carefully planned to spread via viral infections and other malicious software. They use email, social engineering, P2P (peer to peer) networks, and other techniques to spread to

other computers. Once your PC is infected, it may attempt to spread the botnet code to others on a local network in a home or office setting.

Botnets are most often used to spew massive quantities of spam, which is where most of the "enhance your body part," offers and phishing scams come from. But since the botnet code runs with full privileges on the infected computer, it can be used to gather sensitive information from businesses, political groups or governments. Sometimes, the attacks are used to damage or take down a competitor's website by flooding it with emails or web connections. These attacks can be hard to defend against, because the attacking computers are spread all over the Internet. And when the "attacker" is identified, it's just some guy in Podunk who let his anti-virus protection expire, and had no idea his computer was involved in a global crime spree.

Bots can also be used as agents for mass identity theft. This happens through phishing emails that appear to be from a legitimate company in order to convince the user to submit personal information and passwords. Be especially wary of emails claiming to be from eBay, Paypal, banks or the government. Never click on email links to access these sites -- always use your bookmark or key it in directly.

How to Avoid Botnets

The story of the "good hacker" and his botnet illustrates the point that many users take security very lightly, or just don't understand the basics of protecting their computers from online threats. This researcher didn't even have to try very hard. Using only the most common usernames and passwords, he gained access to several hundred thousand routers and other devices. Fortunately, this botnet had no malicious intentions. In fact, it even tried to disable other criminal botnets when they were encountered.

You are most likely to get sucked into a botnet if you do these things:

- Fail to secure your router and wifi with a unique username and password. (See my Wireless Network Security Checklist for details.)
- Fail to secure your computer. (See Ten Steps to Securing Your New PC)
- Fail to use a good spam filter.
- Fail to use firewall protection.
- Click on dubious links in spam emails or shady websites

Use good security practices outlined in the links above, and avoid suspicious emails, especially unexpected messages with subject tags related to holidays, celebrities or current events. Watch out for phishing scams, never click on (or buy!) anything advertised in a spam email, and when in doubt, just don't click.

Fortunately, in the past few years, law enforcement and computer security companies have had some success in tracking down and neutralizing some of the most notorious botnets. In March 2010, the FBI and authorities in Spain busted the Mariposa botnet (over 12 million computers) and arrested the people behind it. In 2011, Microsoft and Kaspersky combined to

neutralize the Rustock and Kelihos botnets. In 2012, the Grum botnet, which was spewing 18 billion spam messages a day, was taken down. And most recently, Microsoft and Symantec teamed up to defeat the Bamital botnet, which was hijacking the web searches of over 8 million users.

How to Detect and Remove Botnet Infections

It's difficult to detect if your computer has been caught up in a botnet, because the software that's implanted is designed to operate in stealth mode. If you notice that your computer is sluggish, that *may* be a sign that you are affected. (For related reading, see How to Speed Up Windows 7.) But in general, if you have been affected by a botnet, you've got some sort of malware infection. Install good anti-virus and anti-spyware software (refer to the links above), and it should detect, take care of, or prevent the problem.

Read more: http://askbobrankin.com/botnet_alert_are_you_vulnerable.html#ixzz2P8DcIWSz

Facebook Phones Home

From; “askbobrankin.com”.

The long-rumored Facebook phone is finally here. Except it's not really a phone. It's YOUR phone, with a new face. But is it a friendly face, or another 'in your face' intrusive reach by Facebook into your privacy? Here's the scoop on Facebook Home, and your phone...

What is Facebook Home?

Mark Zuckerberg wants to be the annoying little brother who followed you everywhere when you were kids. You know, the one who was always in your face, getting in your way while trying to “help”... the one who memorized everything you did and spilled the most awkward parts to your parents and peers... the one you loved but wanted to strangle.

Of course, the founder and CEO of Facebook doesn’t see it that way. He figures that since 25 per cent of online time is spent on Facebook or its subsidiary, Instagram, then it makes perfect sense for Facebook to take over your Android smartphone’s home screen. That is what the company’s new app, Facebook Home, does. Hello, little brother... or is it Big Brother?

Facebook Home replaces your palm-sized desktop of handy apps and icons with a stream of Facebook and Instagram content. Photos of what your Facebook friends are doing stream by constantly. Status updates and messages of dubious

importance roll by. And, of course, there will be ads.

It's very convenient if you bought a smartphone in order to "like" things. But that means other apps like your web browser, Gmail, Maps, Twitter, and Angry Birds will take a back seat. They are still accessible but you have to work a little harder to get past Facebook Home and use them.

Already, the privacy police are speculating about what Facebook Home may or may not be doing in the background. They start with the obvious truism that Mark Zuckerberg wants to know exactly what you're doing every minute of every day, so that he can use that knowledge to increase his ad revenue.

Facebook Home is capable to capturing data about what apps you use and how long you use them. It can tap GPS hardware to figure out where you live (e. g., where does the phone sit without moving all night?) It can tap a phone's accelerometer to deduce when you are jogging. Who knows what Facebook will do with such information, and why would anyone trust Facebook's privacy record?

What's In It For Facebook Users?

Fans of Facebook Home say it adds a third dimension to the traditional side-to-side phone interface, integrating and enriching the user experience. Other apps' notifications, such as "you have mail," pop up and overlay whatever you are doing on Facebook. You don't have to quit a game or app to chat with someone. You never, ever, have to ignore your Facebook friends (or the ads).

A plus for some is that your phone's SMS text messaging and Facebook messaging are unified into a single interface. When Facebook incorporates VoIP calling for "Chat Heads" (Facebook Home's way of displaying your contacts) the virtual mobile life will be complete.

Facebook Home for Android will be available for download on April 12, 2013. Facebook is also partnering with smartphone manufacturers to pre-install the Facebook Home software on some

Android phones. The $99 HTC First (also available starting April 12) will be the first such offering. For now, you won't be able to get Facebook Home on iPhones or iPads. For that to happen, Facebook must convince Apple to make changes to the core of iOS, the Apple operating system for mobile devices.

If you're really into Facebook (and blissfully unconcerned about privacy issues), I can see how Facebook Home might be something you'd like to try. If Facebook is a place you visit only once in a while, to catch up with friends or post an occasional update, it'll seem more like an annoyance than a convenience. No doubt you will be hearing more from Little Brother about the benefits and availability of Facebook Home. Will you try it?

Read more: http://askbobrankin.com/facebook_phones_home.html#ixzz2PynDTK3m

USB speed will double to 10Gbit/s

Standard doesn't have a name yet
By **Mads Oelholm** in the "inquirer.net".
Wed Apr 10 2013, 10:48

BEIJING: THE GROUP behind the USB standard has quietly developed a specification that is set to double USB speed from 5Gbit/s to 10Gbit/s.

At the Intel Developer Conference (IDF) in Bejing, Jeff Ravencraft, president of the USB Implementers Forum (USB-IF) told The INQUIRER that the new specification is nearing completion and should be ready in June.

Ravencraft said that once the specification is complete we will have to wait another nine months before the first discrete controller becomes commercially available, and it probably will be 2015 before the new standard is integrated into chipsets.

The new standard, which has yet to be named, will require a new cable and this will be an all-in-one cable that is capable of handling the new standard as well as power delivery. The cable will also be backwards compatible with the prior versions of the USB standard.

Ravencraft also indicated that there is further headroom in the standard to again double the speed to 20Gbit/s.
The USB-IF has tightened the screws a bit on the logo standard, in that companies will only be allowed to use the logo for the new USB standard if they get their USB product(s) certified.
This doubling of the USB speed might challenge Intel's proprietary Thunderbolt technology that runs at the same speed, though it supports two lanes per port, effectively doubling the aggregate speed. µ

Still Holding on to XP or Windows 7?

From “askbobrankin.com”

Windows 8 is a radically new operating system that many users, consumer and business, are not prepared to adopt. Since its release last Fall, it’s appeared on only three per cent of desktops. If you want to cling to Windows 7 or, more desperately, Windows XP, how long can you do so and what should you expect? Here's the scoop...

How Long Can I Keep My Windows XP or Win7?

Windows 7 users can rest comfortably until at least January 2015. That’s when “mainstream” support of the OS will end, according to Microsoft. Until then, you will continue to receive both security and non-security updates (product enhancements and non-security bug fixes). If your license came with free incident support, you will get it.

But on January 13, 2015, support for Windows 7 will be scaled back. You’ll still get free security-related updates, but patches will be available only by subscription. You will have until April 15, 2015, to buy a subscription to this “extended support.” Warranty claims will not be honored and you will not get new features, only bug fixes.

All support for Windows 7 will end in early 2020, according to Microsoft’s product life-cycle policy. After that, you will receive no security patches and money won’t buy any other support. By then, you'll need a plan to migrate to a newer version of Windows, Mac, Linux, or whatever else is available in 2020.

What About Windows XP?

Windows XP is much closer to becoming an orphan. XP has been in the Extended Support phase since April 14, 2009, and all support will end on April 18, 2014. (Extended support for Vista will end in April 2017.) If you are running XP, you should start planning a migration to Windows 7 or Windows 8 real soon now. It isn't a trivial task, especially for business users.

User data and settings will transfer to a newer operating system fairly easily. But all application software will have to be re-installed. That means you may have to track down CDs, DVDs, downloaded installation files, and license keys. Some applications written for XP will be incompatible with Windows 7 or 8, wholly or in part. You should identify incompatible apps well ahead of time and find alternatives.

Clinging to an orphaned operating system is a foolish and dangerous option, not unlike driving on bald tires or an empty oil reservoir. Malware writers and hackers will increase their targeting of orphaned operating systems and you will receive no defensive patches. Some sort of disaster is virtually guaranteed.

"You'll Have to Pry it From My Cold, Dead Hard Drive..."

If you're still running XP or Windows 7, and you're determined to do so for as long as possible, here are a few pieces of advice:

Use good anti-malware protection. My related articles Lab Tests Reveal Top AntiVirus Programs and Free Anti-Virus Programs will provide some helpful tips.

Have a backup plan. If you have an old operating system, you probably have an old hard drive too. Regular backups will save your bacon if the drive fails, and will also put you in a better position to move on to a new computer or operating system when the time comes. See my tips in Free Backup Software for help with backup strategies.

Start taking inventory. My article What's Going On Inside My PC? will help you identify the hardware and software installed on your computer. If a component inside your dusty old computer fails, you'll have a parts list to help you replace it. You'll also be able to create a handy list of your software license codes, so that when Windows upgrade time finally comes, you can more easily re-install the software you've purchased, without having to buy another copy.

Is It Hard to Move to Windows 8?

The primary complaint about Windows 8 is that the user interface is completely different. Microsoft has decided that the new interface they designed for smartphones, tablets and touchscreen computers should be shoe-horned on all desktop and laptop computers that run Windows 8. The familiar Windows desktop is still there, but it's shoved off in a corner, and they've eliminated the Start button.

Making the leap to Windows 8 is less painful if you can keep the Start button and other familiar user interface features. A number of third-party programs let you do just that. One of them is Windows 8 Start Button http://www.windows8startbutton.com which preserves the Start button; boots your system into the Win 7-like "desktop mode," restores familiar window and menu options, and lets you customize classic Windows and Aero modes. Best of all, it's free. Still, you may face application compatibility issues when upgrading from XP, and to a smaller degree when upgrading from Win 7.

I understand that for many users, there's just no compelling reason to switch from XP or Windows 7, when everything seems to be working fine. Windows 8 will come to them only when they purchase a new computer. I have desktop computers in my home running both XP and Windows 7, and a laptop with Windows 8. Sometime before next April, I'll retire the XP machine, buy a new computer with Windows 8, and restore all my files from backup. As for the XP software I use now, I'll try to find free alternative (preferably web-based) equivalents in the interim. As for the Windows 7 machine, I see absolutely no reason to upgrade.

Read more:
http://askbobrankin.com/still_holding_on_to_xp_or_windows_7.html#ixzz2OaTq12cD

iPhotoDraw 1.6

Use this program to add handy annotations to your favorite digital images. You can add name tags to people found in your photos; provide dimension information for objects seen in your photos; or enlarge and enhance important ...

http://go.infopackets.com/e20130409-17/OkEs75

Ransomware Scam Uses Browser History to Dupe You

By Brandon Dimmel on 20130403 in "infopackets.com".

The only thing worse than a ransomware scam is an informed ransomware scam. According to reports, a new scheme uses a victim's browsing history to construct more believable threats.

Ransomware is malicious software designed to scare Internet users into paying hackers cash.

Ransomware creators achieve this goal by using special software that, once installed, disables critical system functions. The ransomware scammer then tells a victim that, in order to reclaim control of their PC, they must pay up.

Beware Messages From DoJ, DHS, FBI

I Know Who You Are and I Have A Scam Just For You!

A new ransomware scam involves sending victims a fake message supposedly authored by the United States Department of Justice, Department of Homeland Security, or Federal Bureau of Investigation. (Source: times-standard.com)

These messages claim that a victim's computer has been used to access illegal content. In response, the government agency has decided to disable critical system functions on the targeted computer.

Here's what sets this scam apart from the others: in order to make the scam more believable, the scammers use a victim's browser history to show actual websites visited by the victim. They victim is then told that this is where they acquired the illegal content.

The fake message may also list a victim's IP address, lending further credibility to the scammers' claims.

Police-Themed Scams on the Rise

Scams like this are becoming increasingly profitable and popular. According to Kaspersky Lab expert Sergey Golovanov, the number of police-themed ransomware infections has doubled since the beginning of 2013.

Golovanov reminds Internet users to never reply to these kinds of messages.

"What you need to do is go to another computer and start searching for a solution, which you will always be able to find on the Internet," Golovanov said. "All antivirus companies post free instructions and utilities to help users unblock their computers." (Source: pcworld.com)

"In the worst-case scenario, if you are faced with a unique blocker, you can always address the specialized forums of antivirus companies or contact tech support for expert advice and solutions," Golavanov added.

"Of course, this could take some time, but the key thing is not to pay up and fund this extortion."

Quote of the month:

Only Irish coffee provides in a single glass all four essential food groups: alcohol , caffeine, sugar and fat.
-- Alex Levine

Till next month

Your editor: Bob Murray